إجراءات البحث والتحري عن الجريمة المعلوماتية
" الخصوصية والإشكالات "

بن بادة عبد الحليم
طالب دكتوراه تخصص القانون العام الاقتصادي
جامعة غرداية

مقدمة:

بالرغم من المزايا التي تحققت ولا تزال تتحقق كل يوم بفضل تقنية المعلومات على جميع الأصعدة وفي شتى مجالات الحياة المعاصرة، لدرجة حتى أصبحت جميع القطاعات المختلفة تعتمد في أداء عملها بشكل أساسي على استخدام الأنظمة المعلوماتية؛ لما تتميّز به من عنصري السرعة والدقّة في تجميع المعلومات وتخزينها ومعالجتها، ومن تمّ نقلها وتبادلها بين الأفراد والشركات والمؤسسات المختلفة داخل الدولة الواحدة أو بين عدّة دول لهذا صار يطلق على هذا العصر بعصر المعلوماتية.

لكن وعلى الرغم من المزايا الهائلة التي تحققت وتتحقق كما أسلفنا، فإن هذه الثورة التكنولوجية المتنامية صاحبتها في المقابل جملة من الانعكاسات السلبية والخطيرة جرّاء سوء استخدام هذه التقنية، فكطبيعة النفس البشرية غالبا فإن بعض الأشرار يحاولون استغلال المخترعات العلمية وما تقدمه من وسائل متقدّمة في ارتكاب العديد من الجرائم التقليدية مستغلين الإمكانيات الهائلة لهذه المستحدثات، أو إستحدات صور أخرى من الإجرام يرتبط بهذه التقنيات التي تصير محلا لهذه الجرائم أو وسيلة لارتكابها، وقد تزايدت معدلات هذه الجرائم في العقدين الأخيرين بكثرة بصورة أدّت إلى بزوغ فجر ظاهرة إجرامية جديدة تعرف بالإجرام المعلوماتي أو الإلكتروني، حيث يسميها الأستاذ نبيل صقر بجريمة الكمبيوتر ويعرفها كما يلي هي كل سلوك غير مشروع معاقب عليه قانونا صادر عن إرادة جرمية محله معطيات الكمبيوتر.[1]

وعلى ضوء ذلك فإنّ هذه الظاهرة الإجرامية التقنية أثارت العديد من الإشكالات في نطاق قانون الإجراءات الجزائية الذي وضعت نصوصه لتحكم الإجراءات المتعلقة بجرائم تقليدية لا توجد صعوبات كبيرة في إثباتها أو التحقيق فيها وجمع الأدلة المرتبطة بها، وهو ما لا يمكن تصوّره في جريمة ترتكب في بيئة افتراضية تقنية لا تخلف أي أثار مادية محسوسة ولا يرتكبها إلا مجرمون يتسمون بالذكاء والدراية في التعامل مع مجال المعالجة الآلية للمعطيات والإلمام بالمهارات والمعارف التقنية، كما أنّ هذه الجريمة تتم في الخفاء و يعمد مرتكبوها إلى إخفاء أنشطتهم الجرمية عن طريق التلاعب بالبيانات والذي غالباً ما

يتحقق في غفلة من المجني عليه، فضلاً عن سهولة تدمير الدليل ومحوه من مسرح الجريمة مما يعقد أمر اكتشافها وتحديد مرتكبها.

من خلال كل ذلك فإنّ أهم تساؤل يمكن طرحه فيما يتعلق بهذه القضية هو حول مدى صلاحية إجراءات التحقيق والبحث لضبط وإثبات جريمة ارتكبت في عالم افتراضي غير ملموس؟ وهل ذلك سوف يجعل من قانون الإجراءات الجزائية قاصراً عن الوفاء بمتطلبات الشرعية الإجرائية في مواجهة طرق إجرائية في سبيل البحث والتحري عن الجريمة المعلوماتية؟.

لمعالجة مستفيضة لهذه الإشكالية ودراستها من شتى الجوانب، فإنا قد ارتأينا تقسيم هذا المقال إلى مبحثين نتناول فيهما ما يلي:

المبحث الأول: إجراءات الحصول على أدلة إثبات الجرائم المعلوماتية

المطلب الأول: الإجراءات التقليدية للحصول على الدليل المعلوماتي

المطلب الثاني: الإجراءات الحديثة للحصول على الدليل المعلوماتي

المطلب الثالث: القيمة القانونية للدليل المعلوماتي

المبحث الثاني: معوقات البحث والتحري عن الجرائم المعلوماتية

المطلب الأول: المعوقات التقنية

المطلب الثاني: المعوقات البشرية

المطلب الثالث: المعوقات القضائية

المبحث الأول: إجراءات الحصول على أدلة إثبات الجرائم المعلوماتية

نظراً للطبيعة الخاصة التي تتمتع بها الجريمة المعلوماتية؛ كونها جريمة حديثة النشأة وتتمتع بخصوصية من حيث مرتكبها والوسائل المستعملة في ارتكابها والمحل الذي تقع عليه، فإنّه بات لازماً البحث عن إجراءات جديدة تكون أكثر فاعلية في البحث والتحري عن الجريمة المعلوماتية، إذ أنّ وسائل التحقيق التقليدية رغم أنّها لا تزال مستعملة في التحقيق، إلاّ أنّها باتت عاجزة في شكلها الحالي على مواكبة سرعة تطور وسائل الإجرام الإلكتروني ودقته، مما يجعل الأمر ملح إلى إعادة تكييف تلك الوسائل مثل التفتيش والخبرة حتى تتلاءم ومقتضيات التحقيق في مثل تلك الجرائم الغير تقليدية (**مطلب أول**)، ولأنّ المشرّع الجزائري أيقن بأنّ السياسة الجنائية في سبيل القضاء على الجريمة المعلوماتية؛ لن تكون ناجعة ما لم يتم تدعيم جهات البحث والتحري بأدوات ووسائل جديدة تكون متوافقة وطبيعة تلك الجريمة، لهذا قام المشرّع بتدعيم جهات التحقيق بوسائل إجرائية مستحدثة تتفق وعملية البحث عن الدليل الرقمي من حيث طبيعته وطبيعة البيئة التي يتواجد فيها (**المطلب الثاني**)، إلاّ أنّ الفقه قد أثار عدة إشكالات فيما يتعلق بمشروعية الأدلة المتحصّلة عن مثل تلك الجرائم ومدى الاعتداد بها كوسيلة من وسائل الإثبات (**المطلب الثالث**).

المطلب الأوّل : الإجراءات التقليدية للحصول على الدليل الرقمي

من المعلوم أنّ الأنظمة الإجرائية لمختلف الدول تحتوي على مجموعة من الأساليب والوسائل التقليدية التي تلجأ إليها سلطات البحث والتحري للكشف عن مختلف الجرائم مثل الخبرة والتفتيش، حيث تعتبر تلك الوسائل من الأساليب العامة والتقليدية المستعملة للتحقيق في أي جريمة كانت، لدى وباعتبارها أي الجريمة المعلوماتية من الجرائم، فإنّه وجب الاستعانة بتلك الوسائل رغم تقليديتها من أجل التحقيق.
طبعاً ولأنّ البيئة الإجرامية مختلفة والجاني والمجني عليه مختلفان كذلك عن نظيريهما في الجرائم التقليدية، بالإضافة إلى الوسائل المرتكبة بواسطتها الجريمة المعلوماتية، فإنّه أصبح من الضروري إعادة تحيين تلك الوسائل التقليدية بما يتوافق مع الطبيعة الخاصة للجريمة المعلوماتية حتى تتمكن من إنتاج دليل يعتد به قضائيا.

الفرع الأول: التفتيش

يذهب اغلب فقهاء القانون الجنائي إلى القول أنّ التفتيش هو أحد إجراءات التحقيق يباشره موظف مختص بهدف البحث عن أدلة مادية لجناية أو جنحة تحقق وقوعها في محل يتمتع بحرمة خاصّة وذلك وفقاً للضمانات والقيود القانونية المقرّرة.[2]

وهناك من يعرّف التفتيش بأنّه إجراء من إجراءات التحقيق تقوم به سلطة مختصّة لأجل الدخول إلى نظم المعالجة الآلية للبيانات بما تشمله من مدخلات وتخزين ومخرجات لأجل البحث فيها عن أفعال غير مشروعة تكون مرتكبة وتشكل جناية أو جنحة والتوصّل من خلال ذلك إلى أدلّة تفيد في إثبات الجريمة ونسبها إلى المتهم بارتكابها.[3]

يتّضح من خلال التعريفين الأهمية البالغة لهذا الإجراء والخصوصية الكبيرة التي يتمتع بها نظراً لما يمثله من اعتداء على حرمة الحياة والأماكن الخاصّة لهذا قيده المشرّع الجزائري بمجموعة من الضوابط لا من حيث الأوقات التي يتم فيها[4]، ولا من حيث الأماكن التي يمكن أن تخضع للتفتيش[5]، ولا من حيث الجهات المخول لها القيام بعملية التفتيش.[6]

هذا من حيث القواعد العامة للتفتيش إلاّ أنّ التساؤل المطروح هو في مدى ملائمتها وقابليتها للتطبيق على جرائم ذات طبيعة خاصة مثل الجريمة المعلوماتية؟.

للإجابة على هذا التساؤل يجب الخوض في عدّة مساءل يتطلبها التفتيش في شكله العام والتقليدي والمطبق على الجرائم الأخرى، فأوّل تلك المسائل هي مسرح الجريمة، حيث لا يمكن بأيّة حال من الأحوال القيام بعملية تفتيش ما لم نكن أمام مسرح للجريمة، لهذا وجب علينا البحث في ماهية مسرح الجريمة الإلكترونية ومكوناته.

قسم الفقهاء مسرح الجريمة المعلوماتية إلى نوعين، مسرح تقليدي وأخر افتراضي.

– **المسرح التقليدي:** يتمثل هذا المسرح من الجريمة المعلوماتية في الوسائل الموجودة والملموسة في المكان الذي ارتكبت فيه الجريمة مثل أجهزة الإعلام الآلي، أقراص التخزين، الصور، البصمات وبالتالي فهذا المسرح لا يختلف عن المسرح في الجريمة التقليدية.

– **المسرح الافتراضي:** هذا المسرح هو الذي يصنع الفرق والخصوصية بين الجريمة المعلوماتية وباقي الجرائم، كونه تتجلى فيه فنيات وتقنيات ارتكاب الجريمة المعلوماتية ومن خلاله يمكن الحكم على وسائل البحث والتحري التقليدية في ما مدى نجاحها في الكشف عن مثل تلك الجرائم، ويتمثل هذا المسرح في داخل الحاسوب من خلال المكونات الرقمية التي تتواجد فيه وفي مختلف مكوناته (الذاكرة، الأقراص الصلبة...)، ولا يمكن أن يتعامل مع هذا المسرح إلا شخص خبير ذو دراية واسعة بفنيات وتقنيات الحاسب الآلي.

لهذا فإنّ أكثر الإشكالات تطرح عندما يتعلق الأمر بالمسرح الافتراضي للجريمة المعلوماتية بسبب طبيعته وخصائصه التي لا تتفق بتاتاً مع الشروط والقيود التي تتطلبها عملية التفتيش، فمثلا هل يتطلب الأمر الحصول على إذن مسبق بالتفتيش والدخول وحجز الدليل في أحراز كما هو منصوص عليه في التفتيش التقليدي، بالرغم من أنّ المحقّق لن يكون بحاجة إلاّ لمجرد جهاز إعلام ألي موصول بشبكة الانترنت حتى يتمكن من المسك بخيوط الجريمة.

كما أنّ عملية البحث عن الأدلة الرقمية في الكيان المنطقي لجهاز الحاسوب أو في شبكة الانترنت لا تتطلب حضور صاحب المسكن أو المشتبه فيه أو المتهم، لأنّ عملية التفتيش ترتكز على خبرة المحقق وعلى إلمامه بالتقنية المعلوماتية وأنّ حضور صاحب المسكن أو المشتبه فيه أو المتهم أمر لا جدوى منه.[7]

لهذا قام المشرع الجزائري كخطوة منه لملائمة إجراء التفتيش مع متطلبات البحث والتحري في الجريمة المعلوماتية إلى إزالة العقبات التقليدية التي يمكن أن تقف حائلاً أمام المحقق في الجريمة المعلوماتية من خلال نصه على أنّه: " **يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة 04 أعلاه الدخول بغرض التفتيش ولو عن بعد إلى:**

– منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها.

– منظومة تخزين معلوماتية.

في الحالة المنصوص عليها في الفقرة " أ " من هذه المادة إذا كانت هناك أسباب تدعو للاعتقاد بأنّ المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى وأنّ هذه المعطيات يمكن الدخول إليها، انطلاقا من المنظومة الأولى ، يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا بذلك ".[8]

يمكن من خلال ذلك إثارة أهم إشكالين يعترضان إجراء التفتيش في الجريمة المعلوماتية والذين هما:

- مدى صلاحية الحاسوب كمحل للتفتيش:

أثارت هذه النقطة جدلاً فقهياً واسعاً بين من أيّد فكرة تفتيش الحاسوب ومكوناته مستنداً إلى أنّ إصدار الإذن بالتفتيش يجب أن يفهم بمفهوم واسع يمتد إلى البيانات الإلكترونية بمختلف أشكالها المحسوسة وغير المحسوسة، بينما ذهب رأي أخر إلى القول بأنّه لا ينطبق المفهوم المادي على بيانات الحاسوب غير المرئية أو غير الملموسة وأن المشرّع يجب عليه أن ينص على صراحة على تفتيش المواد المعالجة عن طريق الحاسوب أو بيانات الحاسوب حتى لا يخرج على مبدأ الشرعية.

وذهب رأي ثالث إلى القول أنه بغض النظر عما إذا كان مفهوم الشيء يشمل بيانات الحاسوب أو لا، فإنّ الضبط يجب أن يقع عليها متى إذا اتخذت شكلاً ماديا.[9]

إنّ المتأمل لتلك الآراء الفقهية يمكنه القول أنّ إمكانية التفتيش عن الكيانات المعنوية في الحاسوب صارت واردة وحتمية ومعترف بها، إذ أنّ الكيانات المعنوية وإن كانت غير مادية إلاّ أنها تدخل في نطاق الأشياء المادية، بالإضافة إلى التطور الحاصل في وسائل التفتيش، بحيث أنّها أصبحت لا تقف عند الأدوات المادية المستخدمة في ارتكاب الجريمة أو ضبط جسم الجريمة الذي يحقّق نموذجها القانوني، وإنما يمكن لتلك الطرق كذلك أن تتعامل مع الجرائم التي ترتكب بواسطة الوسائل الإلكترونية كالحاسوب أو تقع عليه، فيمكن تبعاً لذلك تسجيل بيانات المعالجة آلياً بعد تحويلها من نبضات أو ذبذبات أو إشارات أو موجات كهرومغناطيسية إلى أشياء تسجّل وتخزن على وسائل معينة وعلى تلك الوسائل يرد التفتيش.[10]

- مدى خضوع أجهزة الحاسوب والأنظمة المعلوماتية للتفتيش عن بعد

إنّ التطوّر الحاصل والمذهل في شبكة المعلومات وما أنتجه من تواصل بين مختلف أقطار العالم لدرجة جعل الكرة الأرضية قرية واحدة، ذلك الأمر كانت له تداعيات سلبية، حيث استغل مجرمو الانترنت تلك الإيجابية وحوّلوها إلى نقطة إيجابية في مجال إجرامهم حيث أضفوا على الجريمة المعلوماتية صفة العابرة للحدود إذ صارت الجريمة ترتكب في بلد ونتيجتها تقع في بلد أخر ووسائل ارتكابها في بلد ثالث، كل ذلك جعل سلطات البحث والتحري في ذهول وحيرة من أمرها خاصة في ما يتعلق بالتفتيش، فهل يا ترى من الممكن الوصول إلى تلك البيانات من خلال حواسيب تقع في الموقع الجاري تفتيشه وأنّ تلك البيانات قد تكون موجودة داخل اختصاص قضائي أخر أو في بلد أخر، لهذا ظهرت فكرة التفتيش عن بعد، ولتوضيح ذلك نتطرق لاحتمالين:

الاحتمال الأول: في حالة اتصال حاسوب المتهم بحاسوب شخص أخر غير متهم داخل الدولة

ذهبت مختلف التشريعات المقارنة إلى الاعتراف بحق سلطات البحث والتحري إلى تمديد اختصاصاها في التفتيش حتى إلى حواسيب الأشخاص الغير متهمين وذلك وفق الضوابط التالية:

– إذا كان ضرورياً لكشف الحقيقة بشأن الجريمة محل البحث.

– إذا وجدت مخاطر تتعلق بضياع بعض الأدلة نظراً لسهولة عملية محو أو إتلاف أو نقل البيانات محل البحث.

الاحتمال الثاني: اتصال حاسوب أخر موجود خارج الدولة

ذهب الفقه إلى أنّ التفتيش الإلكتروني العابر للحدود يجب أن يتم وفق الاتفاقيات الثنائية بين الدول من أجل السماح بذلك ولا يجوز القيام بالتفتيش العابر للحدود في غياب تلك الاتفاقيات أو على الأقل الحصول على إذن من الدولة الأخرى.

يمكننا أن كتوضيح لدور الضبطية القضائية في التفتيش اقتباس هذا المقال من جريدة الشروق اليومي الجزائرية والذي جاء فيه " **أن مصالح الدرك الوطني قد شرعت في إجراء تحقيقات دقيقة، حول ظاهرة خطيرة اكتسحت المجتمع الجزائري، تتعلق بجرائم التشهير والابتزاز والمساومة وتشويه السمعة، عن طريق استعمال شبكة التواصل الاجتماعي "الفايس بوك"، وذلك من خلال تجنيد ما يطلق عليهم بـ"دركيو الانترنيت" للإيقاع بالمتورطين في مثل هذه القضايا باستخدام أحدث تكنولوجيات البحث والتحري في الجرائم الالكترونية.**

- بهذا الصدد، أكد قائد فصيلة الأبحاث بالدرك الوطني بالعاصمة لـ"الشروق"، أن قيادة الدرك استحدثت فرقة خاصة أطلق عليها اسم "**دركيو الانترنيت**" تابعين لفرقة البحث والتحري، مهمتها فضح الجرائم الالكترونية عن طريق ما يسمى بالتفتيش الإلكتروني بواسطة تنشيط دوريات أمنية الكترونية، وذلك بعد تفشي ظاهرة نشر صور وابتزاز المواطنين عن طريق شبكة التواصل الاجتماعي، إلى جانب إتلاف المواقع الالكترونية الخاصة بالمؤسسات الخاصة والحكومية.
- على هذا الأساس طلب نفس المسؤول، من المواطنين بوجوب تقديم شكوى في حال التعرض لهذا النوع من الجرائم التي تستهدف المساس بحرماتهم الشخصية، مؤكدا أن مصالح الدرك تعمل جاهدة للتصدي لهذا النوع من الجرائم.
- وعن العقوبات التي ستطبق على أصحاب جرائم "الفايس بوك" خصوصا والجرائم الإلكترونية عموما، أكد المحامي بوجمعة غشير في اتصال مع "الشروق" أن المتورطين في مثل هذه القضايا سيعاقبون على شاكلة المجرمين المتورطين في القضايا الأخرى، أي ما يعرف بالجرائم الورقية، حيث ستسلط عقوبة تتراوح ما بين سنتين و5 سنوات حبسا، زيادة عن المبالغ المالية التي يحددها القاضي حسب درجة خطورة القضية.
- وفي سياق الشروع في التصدّي لجرائم "الفايس بوك" ومعاقبة المتورطين، عالجت فصيلة الأبحاث والتحري التابعة للدرك الوطني بالعاصمة، أول قضية من نوعها تتعلق بابتزاز المواطنين عن طريق "الفايس بوك"، حيث تمكنت من الإيقاع بشاب إبتز فتاة عن طريق نشر صورها في

وضعيات حرجة بعد أن رفضت طلبه للزواج بها، مستخدما خط الانترنيت اللاسلكي المعروف بـ"الويفي" من عند جاره الذي منحه الرقم السري لدخول الانترنيت.

- تفاصيل هذه القضية حسب قائد فصيلة الأبحاث بالدرك الوطني بالعاصمة، تعود إلى شهر ماي لما تقدمت شابة تبلغ من العمر 24 سنة إلى مقر الفصيلة لإيداع شكوى ضد مجهول، الا أنها وجهت أصابع الاتهام لصديقها السابق البالغ من العمر 26 سنة، واتهمته بنشر صور لها في وضعيات مخلة بالحياء عبر شبكة "الفايس بوك"، حيث يتقاسم الصفحة مع حوالي 1000 شخص، وأصبح يبتزها بهذه الصور باستعمال تقنيات "الفوتوشوب"، حيث كان يستعمل صور نجمات الإغراء وهم في وضعيات مخلة بالحياء، وباستعمال تقنية التركيب يأخذ صورة الضحية ويضعها على جسد إحدى هذه النجمات العاريات، والسبب في ذلك هو رفض هذه الأخيرة الارتباط به، نظرا لفارق المستوى التعليمي بينها وبينه، كما أصبح يرسل لها صورها "المخلة بالحياء" إلى بريدها الالكتروني باستعمال بريد جديد.
- وفور ذلك باشر "**دركيو الانترنيت**" الذين تلقوا تكوينا خاصا في كيفية الوصول إلى المجرم الإلكتروني، تحقيقات معمقة للتوصل إلى المتهم وذلك باستعمال أحدث تقنيات البحث والتحري لفضح المشتبه فيه، حيث دام البحث 20 يوما فقط، وبعد جمع كل الأدلة، تم تفتيش منزله الكائن العاصمة، أين تم العثور داخله على جهاز الإعلام الخاص به وصور الفتاة إلى جانب الرسائل التي كان يبعث بها عن طريق "الفايس بوك"، إلى جانب أجهزة عسكرية تعود للفترة التي قضى فيها مدة خدمته العسكرية.
- هذا، وقد تم تقديم المجرم إلى وكيل الجمهورية لمحكمة الشراقة، الذي أمر إيداعه الحبس المؤقت بالحراش بعد أن وجه له تهمة النشر والتشهير بالصور الفوتوغرافية عن طريق الانترنيت وعرض صور مخلة بالحياء.
- من جهة أخرى، تقدم مدير إحدى الجرائد الوطنية، إلى مقر فصيلة الأبحاث والتحري التابعة للدرك الوطني بالعاصمة، لإيداع شكوى ضد مجهول قام بتخريب الموقع الإلكتروني لجريدته، الأمر الذي تعذر على القراء تصفح مضامين الجريدة لمدة تزيد عن 3 أيام.
- كما تقدم أحد الإطارات السامية من ذات المصالح لإيداع شكوى ضد مجهول حاول تشويه سمعته عبر صفحات "الفايس بوك"، مما سبب حرجا له أمام كل من يعرفه حتى خارج الوطن.[11]

الفرع الثاني: الخبرة

الخبرة القضائية هي وسيلة من وسائل الإثبات يتم اللجوء إليها إذا اقتضى الأمر كشف دليل أو تعزيز أدلة قائمة، كما أنها تعتبر استشارة فنية يستعين بها القاضي أو المحقق في مجال الإثبات

لمساعدته في تقدير المسائل الفنية، التي يحتاج تقديرها إلى دراية علمية لا تتوافر لدى عضو السلطة القضائية المختص بحكم عمله وثقافته.[12]

إنّ الطبيعة الخاصة للجريمة المعلوماتية تجعلها من أكثر الجرائم لجوءا إلى الخبرة من أجل كشف ملابساتها وفك خيوطها نظراً لضعف جهات التحقيق والقضاء في هذا المجال، وإذا كانت الخبرة التقنية في مجال التعاون القضائي تعتبر من أبرز مظاهر التعامل القانوني والقضائي مع ظاهرة تكنولوجيا المعلومات والانترنت، خاصّة إزاء نقص المعرفة لدى القانونيين بظاهرة تقنية المعلومات، لهذا فهل يمكن أن تعترض الخبرة التقنية مبدأ " **القاضي خبير الخبراء** " لهزّات عنيفة إزاء التزايد المتواصل لمبدأ التفاعل القانوني مع ظاهرة البيئة الرقمية التي تقع في اختصاص أخر غير الجوانب النظرية القانونية التي لا تسمح ثقافة القاضي المبنية على معايير الدراسات القانونية من التفاعل معها.[1413]

– **متطلبات أعمال الخبرة في مجال الجريمة المعلوماتية:** نظرا للخصوصية الفنية والعلمية للخبرة في مجال الجريمة المعلوماتية فإنه ينبغي على الخبير الإلمام بالمواضيع الآتية:

– الإلمام بتركيب الحاسوب وصناعته وطرازه وطريقة تشغيله.

– طبيعة البيئة التي يعمل في ظلّها الحاسب.

– القدرة على أداء المهام دون أن يترتب على ذلك إعطاب وتدمير الأدلة المتحصلة من الوسائل الالكترونية.

– التمكن من نقل أدلة الإثبات غير المرئية وتحويلها إلى أدلة مقروءة أو المحافظة على دعامتها لحين القيام بأعمال الخبرة بغير أن يلحقها تدمير أو إتلاف.

– معرفته لوسائل وطرق فحص نظام الحاسب الآلي كبرامج كشف وإزالة الفيروسات وبرامج استرجاع البيانات والمعلومات وإصلاح التالف وإظهار المخفي منها.

– **الأساليب الفنية في عمل الخبير المعلوماتي في اكتشاف الدليل الرقمي**

للخبير المعلوماتي في سبيل تحري الحقيقة أن يقوم بكل ما يمكنه من التوصل إليها وهو إطار القيام بعمله له أن يستخدم الأساليب التي يقوم عليها تخصصه وليس للمحكمة أن ترفض تلك الأساليب ما لم يكن رفضها لها مسببا بشكل منطقي.

ويرى بعض المختصين أنّ عمل الخبير المعلوماتي في اشتقاق وتجميع الأدلة الرقمية يتم عبر ثلاث مراحل:

– **المرحلة الأولى:** تجميع المعلومات المخزّنة لدى الطرف مقدّم الخدمة من خلال تتبع الحاسبات الخادمة التي دخل منها المجرم المعلوماتي ومحاولة إيجاد اثر له.

– **المرحلة الثانية:** مرحلة المراقبة ويتم ذلك بطرق مختلفة أهمها استخدام برامج مراقبة يمكن تحميلها للبحث عن المعلومات المشتبه فيها وحصر وتسجيل بيانات كل دخول وخروج بالموقع.

– **المرحلة الثالثة:** فحص النظام المعلوماتي المشتبه فيه بعد ضبطه من طرف جهات التحقيق بمكوناته المادية والمعنوية لاشتقاق الدليل وتقديمه لجهات التحقيق وتقرير مدى وقوع الجريمة باستخدام النظام المضبوط من عدمه.

كما تجدر الإشارة إلى أنّ المشرّع الجزائري قد نص في المادة 143 من قانون الإجراءات الجزائية في فقرتها الأولى على " **انه يجوز لكل جهة قضائية تتولى التحقيق أو تجلس للحكم إذا تعرّض لها مسالة ذات طابع فني أن تأمر بندب خبير إمّا بناءاً على طلب النيابة العامة أو التحقيق أو الخصوم أو من تلقاء نفسها** ".

من خلال نص المادة 143 يتضح أنّ الاستعانة بالخبير أمر جوازي، إلاّ انه يمكن القول أنّ المسائل الفنية التقنية المتعلقة بالجريمة المعلوماتية فإنّ نذب الخبير فيها أمر لا بدّ منه، حيث تتعلق بمسائل فنية بالغة التعقيد ومحل الجريمة فيها مادّي والتطور في أساليب ارتكابها سريع ومتلاحق ولا يكشف غموضها إلاّ متخصص وعلى درجة كبيرة من التمييز في مجال تخصصه، فإجرام الذكاء والفن لا يكشفه ولا يحل محله إلا ذكاء وفن مماثلين.[15] كما يجب على القاضي اختيار الخبراء من ذوي الإمكانيات العلمية والمقدرة الفنية العالية.

تجدر الإشارة إلى أنّ من بين التشريعات السباقة التي نظمت أعمال الخبرة في مجال الجرائم المعلوماتية القانون البلجيكي الصادر في 23 نوفمبر سنة 2000[16]، حيث نصت المادة 88 منه على أنه يجوز لقاضي التحقيق والشرطة القضائية أن تستعين بخبير ليقدّم وبطريقة مفهومة المعلومات اللاّزمة عن كيفية تشغيل النظام وكيفية الدخول فيه أو الدخول للبيانات المخزنة أو المعالجة أو المنقولة بواسطته، ويعطي القانون كذلك لسلطة التحقيق أن تطلب من الخبير تشغيل النظام أو البحث فيه أو عمل نسخة من البيانات المطلوبة لتحقيق أو سحب البيانات المخزنة أو المحولة أو المنقولة على أن يتم ذلك بالطريقة التي تريدها جهة التحقيق.[17]

المطلب الثاني: إجراءات البحث والتحري الحديثة

أمام عجز وسائل التحقيق التقليدية في البحث والتحري عن الجريمة المعلوماتية كان لزاماً على مختلف التشريعات الحديثة إلى أن تبحث عن وسائل أكثر ملائمة مع الطبيعة الخاصة للجريمة المعلوماتية، حتى تتحقق تلك النتيجة المرجوة من التحقيق، ولأنّ المشرّع الجزائري قد استشعر ذلك ومدى خطورته على البحث والتحري عن الجريمة المعلوماتية، لجأ إلى انتهاج خطّة محكمة واضحة المعالم في مكافحة الجريمة المعلوماتية، حيث كانت أولى نتائج تلك السياسة ما جاء في القانون 22/06 المؤرخ في 2006/12/20 المعدل والمتمم لقانون الإجراءات الجزائية وذلك من خلال كل من إجرائي التسرب واعتراض المراسلات، تم من خلال القانون 04/09 والذي قام بموجبه باستحداث إجراء المراقبة الالكترونية.

الفرع الأول: التسرب واعتراض المراسلات

الجريمة المعلوماتية أو الالكترونية هي من بين الجرائم التي يمكن اللجوء فيها لأسلوب التسرب و اعتراض المراسلات إذا دعت ضرورة التحقيق لذلك.

– **التسرب:** تعتبر الجريمة الماسّة بأنظمة المعالجة الآلية للمعطيات من بين الجرائم التي تناولتها وعدّتها المادة 65 مكرر 5 من قانون الإجراءات الجزائية والتي يجوز فيها اللجوء إلى أسلوب التسرب.

والتسرب هو تلك العملية التي يقوم بموجبها ضابط الشرطة القضائية بالتوغل داخل المجموعات الإجرامية وإيهامهم بأنه شريك معهم أو خاف وذلك من اجل الإيقاع بهم.

ومن المعلوم فإنّ التسرّب يخضع لعدة شروط شكلية وموضوعية في حالة مخالفتها يحكم على العملية بالبطلان، وقد تناولت تلك الإجراءات بالتفصيل المواد من 65 مكرر 11 إلى 65 مكرر 15 لهذا لا يمكن التفصيل فيها نظراً لأنه ليس محلها هنا.

ويمكن افتراض عملية التسرب في مجال الجريمة المعلوماتية من خلال قيام ضابط أو عون الشرطة القضائية بالتوغل والدخول إلى العالم الافتراضي وذلك باختراقه لمواقع معينة وفتح ثغرات الكترونية فيها، أو اشتراكه في محادثات غرف الدردشة أو حلقات الاتصال المباشر مع المشتبه فيهم والظهور بمظهر ذلك الفاعل معهم والمشارك، مستخدما الأسماء والصفات المستعارة والوهمية من اجل الإيقاع بهم.

– **اعتراض المراسلات:** جاء في المادة 03 من القانون 09–04 انه مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات والاتصالات يمكن لمقتضيات حماية النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية الجارية وفقاً للقواعد المنصوص عليها في قانون الإجراءات الجزائية وفي هذا القانون، وضع ترتيبات تقنية لمراقبة الاتصالات الالكترونية وتجميع وتسجيل محتواها في حينها و القيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية.

وإن كانت المراسلات تتمتع بالخصوصية التي حماها المشرّع بسن قوانين تعمل على توفير قدر كبير من الحماية الجزائية لها، إلاّ أنّ هذا الأمر لم يكن على الإطلاق، بل قام المشرّع بالسماح باعتراض المراسلات وكشف السرية عنها وذلك إذا اقتضت ضروريات التحري في الجريمة المتلبس بها أو التحقيق الابتدائي في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، ويعتبر هذا هو السند الشرعي المبرر لإباحة هذا الإجراء بسبب انه يشكّل اعتداء صارخ على حرمة الحياة الخاصة وسرية المراسلات فيباح استثناءاً وفي حدود ضيّقة وذلك للفائدة المنتظرة منه والتي تتعلق بإظهار الحقيقة وكشف الغموض عن الجريمة وضبط الجناة.[18]

وتبرز عمليات اعتراض المراسلات أكثر في مجال المراسلات الالكترونية أو البريد الالكتروني بخدمة قائمة التراسل (mailinglist)، وهو نظام تراسل جماعي يمنح صلاحية بث رسالة إلى مجموعة من

الأشخاص المسجلين في القائمة ويحتوي البريد الالكتروني برامج متخصصة لكتابة الرسائل الالكترونية وإرسالها استعراضها وتخزينها.

وتخضع عملية اعتراض المراسلات إلى مجموعة من الشروط والضوابط مثل:

– ترخيص السلطة القضائية ومراقبتها لعملية التنفيذ.

– تحديد طبيعة المراسلة ومدة الاعتراض.

الفرع الثاني: المراقبة الالكترونية

هذا الإجراء تمّ استحداثه بموجب المادة 03 من القانون 04/09 المتضمّن القواعد الخاصّة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتهما، أجاز تبعاً لمستلزمات التحريات والتحقيقات القضائية الجارية في إطار هذا النوع من الجرائم، اللجوء إلى وضع ترتيبات تقنية لمراقبة الاتصالات الالكترونية وتجميع وتسجيل محتواها.

المشرّع الجزائري لم يعترّض لتعريف المقصود بالمراقبة الالكترونية مثله مثل باقي التشريعات، إلاّ أنّ الفقه قد تصدّى لذلك وعرّفه بأنه إجراء مراقبة شبكة الاتصالات، أو هو العمل الذي يقوم بموجبه المراقب باستخدام التقنية الالكترونية لجميع معطيات ومعلومات عن المشتبه فيه سواء أكان شخصاً أو مكاناً أو شيئاً حسب طبيعته مرتبط بالزمن لتحقيق غرض امني أو لأي غرض أخر.

إجراء مراقبة الاتصالات الالكترونية؛ هو إجراء يدخل كذلك في إطار التدابير الوقائية من الجرائم التي يمكن أن ترتكب بواسطة المعلوماتية.

فإلي جانب إمكانية القيام بإجراء مراقبة الاتصالات الالكترونية في إطار التحريات والتحقيقات القضائية من اجل الوصول إلى أدلة لم يكن بالمقدور الوصول إليها لولا استعمال هذه الوسيلة، بالإضافة إلى انه يمكن استغلال هذه التقنية للعمل في بيئة الرقابة من اجل الوقاية من احتمال وقوع جرائم خطيرة بواسطة المعلوماتية من شأنها تهديد كيان الدولة[19]، وهو ما قرّرته المادة الرابعة من القانون 04/09 من خلال نصّها على انه يمكن القيام بعمليات المراقبة الالكترونية للاتصالات للوقاية من الأفعال الموصوفة بجرائم الإرهاب والتخريب والجرائم الماسة بأمن الدولة، وكذا توفّر معلومات حول إمكانية الاعتداء على منظومة معلوماتية على نحو يهدد النظام العام والدفاع الوطني.

يجب الاعتراف للمشرّع الجزائري انه قد قام بخطوة جريئة من خلال نصه على إجراء الرقابة الالكترونية للاتصالات، على اعتبار انه من اخطر الإجراءات في النظام الإجرائي عبر العالم الافتراضي كونه يمس بخصوصية الإنسان وحرمة حياته.[20]

المطلب الثالث: القيمة القانونية للدليل الرقمي

لقد تعامل الفقه والقضاء بريبة اتجاه القيمة القانونية للدليل الرقمي، مخافة أن يكون غير صادق في تعبيره عن الحقيقة المرجوّة من التحقيق بالإضافة كذلك لخصوصية الوسائل التي تمّ بها الحصول

عليه، وما يمكن أن تتعرّض له من تزييف وعبث، لهذا فانه من الواجب التطرّق لمشروعية الدليل الرقمي وحجيته أمام القضاء تم التعريج إلى موقف المشرع الجزائري من كل ذلك.

الفرع الأول: مشروعية الدليل الرقمي وحجيته

– **المشروعية:** هي ذلك التوافق والتقيّد بأحكام القانون بهدف تقرير ضمانة أساسية وجدية للأفراد من اجل حماية حرياتهم وحقوقهم ضد التجاوزات في غير الحالات التي رخص فيها القانون بذلك؛ حماية للنظام الاجتماعي وبنفس القدر تحقيق حماية مماثلة للفرد ذاته.[21]

لهذا فانه من المقرّر أنّ الإدانة في أي جريمة لابد وأن تكون مبنية على أدلة مشروعة تم الحصول عليها وفق قواعد الأخلاق والنزاهة واحترام القانون، وعليه فإنّ الإجراءات التي تم بموجبها جمع الدليل الرقمي المتحصّل من الوسائل الالكترونية إذا خالفت القواعد الإجرائية التي تنظّم كيفية الحصول عليها، فإنها تكون باطلة وبالتالي بطلان الدليل المستمد منها ولا تصلح لأن تكون أدلة تبنى عليها الإدانة في المواد الجنائية.

وهو ما قضت به هولندا في هذا المجال، حيث ألزمت بمحو بيانات الحاسوب المسجلة في ملفات الشرطة في حالة ما إذا كانت غير قانونية، ودعت إلى عدم استعمالها كدليل في الإثبات مثل الحصول على دليل رقمي من خلال إجراء مراقبة الاتصالات دون أن يكون محلاً لإذن من السلطة القضائية المختصة، أو اتخاذ ترتيبات تقنية من أجل تفتيش منظومة معلوماتية تؤدّي إلى المساس بالحياة الخاصّة للغير أو ممارسة الإكراه المادي أو المعنوي في مواجهة المشتبه فيه من أجل فك شفرة نظام من النظم المعلوماتية، أو التحريض على ارتكاب الجريمة من طرف الضبطية، بالإضافة كذلك إلى استعمال الطرق غير المشروعة مثل استعمال الغش والتدليس والخداع في الحصول على الأدلة الرقمية.[22]

– **الحجية:** الدليل الرقمي ما هو إلاّ تطبيق من تطبيقات الدليل العلمي بل وأكثر منه حجية في الإثبات؛ بسبب ما يتميز به من موضوعية وحياد وكفاءة، وهو محكم وفق قواعد علمية حسابية قاطعة لا تقبل الشك والتأويل وهو الأمر الذي يعطه قوة اكبر من حيث الإثبات ويجعل القاضي في امن من الأخطاء القضائية، ويقربه نحو تحقيق العدالة بشكل أكبر نظراً لما يتميز به من دقّة في جمع أدلة تتمتّع بقوّة علميّة يصعب إثبات عكسها، إلاّ أنّ ذلك لا ينفي البتّة استبعاد أن يكون موضوع شك من حيث سلامته من العبث من ناحية، وصحة الإجراءات المتّبعة في الحصول عليه من ناحية أخرى، حيث يمكن أن يشك في صحته من ناحيتين:

الأولى: إمكانية تعرّضه للعبث والخروج به على نحو يخالف الحقيقة.

الثانية: نسبة الخطأ في الحصول على الدليل الرقمي وذلك راجع للخطأ في استخدام الأداة المناسبة في الحصول على الدليل الرقمي.

لهذا فإنّ الشك في الدليل الرقمي لا يتعلّق بمضمونه بل في عوامل مستقلة عنه لأنها تؤثّر في مصداقيته، لهذا أدرجت أغلب التشريعات إلى وجوب توفّر مجموعة من الشروط في الدليل الرقمي من أجل اقترابه نحو الحقيقة وقبوله كدليل في الإثبات الجنائي ومن تلك الشروط:

- وجوب يقينيّة الأدلة الرقمية وغير قابليتها للشك.
- وجوب مناقشة الأدلة الرقمية المستخرجة من الحاسوب.

يمكن القول أنّ مجرّد توافر الدليل الرقمي لا يعني أنّ القاضي ملزم بالحكم بموجبه مباشرة سواء بالإدانة أو البراءة، فالدليل الرقمي ليس آلية معدّة لتقرير اقتناع القاضي بخصوص مسألة غير مؤكّدة إلاّ أنّ ذلك لا ينفي أن نعدم جانب السلطة التقديرية للقاضي، إذ يجب أن يبقى هو المسيطر على حقيقة القضايا المعروضة أمامه، لأنه من خلال سلطته التقديرية يستطيع أن يفسّر الشك لصالح المتّهم وأن يستبعد الأدلة التي تمّ الحصول عليها بطرق غير مشروعة وضرورية أكثر من أجل جعل الحقيقة العلمية قضائية.[23]

الفرع الثاني: موقف المشرع الجزائري من الدليل الرقمي

نصّت المادة 212 من قانون الإجراءات الجزائية، على انه يجوز إثبات الجرائم بأي طريقة من طرق الإثبات وللقاضي أن يصدر حكمه تبعاً لاقتناعه الخاص، كما نصّت المادة 307 من قانون الإجراءات الجزائية أيضاً " **إنّ القانون لا يطلب من القضاة أن يقدموا حساباً عن الوسائل التي بها قد وصلوا إلى تكوين اقتناعاتهم وأن يبحثوا بإخلاص ضمائرهم في أي تأثير قد أحدثته في إدراكهم الأدلة المسندة للمتهم....**".

من خلال تلك النصوص القانونية يتضح جلياً، أنّ المشرّع الجزائري قد تبنى كقاعدة عامة نظام الاقتناع الشخصي للقاضي، بالإضافة إلى فتح المجال أمام أي دليل يمكن من خلاله إقامة الحجة حتى ولو كان دليل رقمي، إلا استثناءاً نجده قد أخذ أيضا بنظام الأدلة القانونية في إثبات بعض الجرائم أين يشترط لإثباتها أدلة قانونية محدّدة مسبقاً وعلى سبيل الحصر.[24]

المبحث الثاني: مظاهر الصعوبة في إثبات الجريمة المعلوماتية

لقد لاقت إجراءات البحث والتحري عن الجريمة المعلوماتية مشاكل وتحديات كثيرة تختلف في جوانب عديدة عن التحديات والمشاكل التي ترتبط بالجرائم التقليدية، وتتمثّل أهم الصعوبات التي تعترض الجهات المكلّفة بالتحقيق في أنّ تلك الجرائم ترتكب في نطاق الأنظمة المعلوماتية وشبكة الانترنت؛ ومحلها هو معلومات وبرامج معالجة آلياً عن طريق الحواسيب أو جرائم تتعلق بالأشخاص عبر عالم افتراضي غير متناهي وغير محدود، الأمر الذي يمنحها طابع خاص ليس فقط في طريقة ارتكابها بل كذلك في الوسيلة التي ترتكب بها؛ فبالرّغم من الجهود الكبيرة التي يبدلها المشرّعين وسلطات التحقيق والضبطيّة القضائية سواء أكانت دولية أو داخلية، إلاّ أنها تصطدم دائماً بعدّة عراقيل وصعوبات ومعوقات

يمكن تقسيمها إلى معوقات لأسباب تقنية (**المطلب الأول**)، وأخرى بشرية (**المطلب الثاني**)، وأخرى قانونية (**المطلب الثالث**).

المطلب الأول: معوّقات تعود لأسباب تقنية

تنقسم هذه المعوّقات في نوعين: الأولى تحول دون اكتشاف الجريمة (**الفرع الأول**)، والثانية تؤدي إلى صعوبة إثباتها (**الفرع الثاني**).

الفرع الأول: المعوّقات المرتبطة بصعوبة اكتشاف الجريمة

تتمثل أهم تلك المعوقات في ما يلي:

– **عدم وجود أثار مادية للجريمة:** الطبيعة الخاصة لهذه الجريمة جعلتها لا تشبه باقي الجرائم في طرق تحريك الدعوى العمومية مثل الشكوى وما إلى ذلك، الأمر الذي جعل أمر اكتشافها من قبل السلطات المعنية صعباً نوعاً ما، وبقاء أغلب تلك الجرائم مجهول لعدم التبليغ عنه، بالإضافة إلى أنّ مرتكب الجريمة المعلوماتية قد يلجأ في غالب الأحيان إلى بدل أقصى احتياطاته لعدم ترك أثار لفعلته، مثل الجرائم المعلوماتية التي تتم دون أن يشعر بها القائمون على تشغيل الأجهزة المعلوماتية؛ كجرائم التجسس التي تتم عن طريق برامج التجسس الخاصة، بالإضافة إلى عدم دراية أغلب مستعملي المعلوماتية ببرامجها، فلا ربما يساهمون بجهلهم وبدون قصد في مساعدة مرتكبي تلك الجرائم بطريقة غير مباشرة، من خلال تثبيت برامج تجسس أو برامج ضارّة بالجهاز أو الضغط على روابط مفخخة، بالإضافة إلى أننا نتعامل أمام عالم افتراضي مسرحه هو المواقع والأجهزة الإلكترونية التي يمكن فيها الحذف والزيادة والتعديل والنقصان فلسنا أمام وثائق ومستندات ملموسة مثل الجريمة التقليدية لنسوق هنا قول الأستاذة نهلا عبد القادر المومني التي قالت بان الجريمة المعلوماتية تتميز بصعوبة اكتشافها وإذا اكتشفت فان ذلك يكون بمحض الصدفة عادة، حيث يبدو من الواضح أنّ عدد الحالات التي تم فيها اكتشاف هذه الجرائم قليلة إذا قورنت بما يتم اكتشافه من الجرائم التقليدية.[25]

– **الطبيعة المتعدّية للحدود الجغرافية التي تتمتع بها الجريمة المعلوماتية:** ساهمت شبكة الانترنت في جعل العالم قرية واحدة؛ من خلال تبادل المعلومات وانتقالها في اللحظة والحين ومن خلال التواصل بين مختلف جهات المعمورة، إلاّ أنّ ذلك رغم طابعه الايجابي فإنه قد تحوّل إلى جانب سلبي استغله مجرمو المعلوماتية وحولوه إلى ميزة لهم لارتكاب أفعالهم الإجرامية؛ التي تعدّت الحدود الجغرافية التقليدية للدول، فمثلاً يكون المجرم المعلوماتي في دولة ويخترق حساب أو موقع مصرف أو بنك في دولة ثانية، ويقوم بتحويل مبالغ أو عمولات إلى دولة ثالثة، بالإضافة إلى ما تتمتع به الجريمة المعلوماتية في أنّ المجرم يبقى قابعاً في مكانه دون أن يتحرك لكسر الإقفال أو خلع الأبواب أو ترك البصمات أو تحويل المسروقات و متحصلات الجريمة، بل يكفيه فقط جهاز كمبيوتر حديث وخط انترنت حتى يصول ويجول في مختلف أنحاء العالم مرتكبا لجرائمه.

تعدّ كذلك شبكة الانترنت بطبيعتها عالمية الهوية والانتشار، وبناءا على ذلك فكل نشاط إجرامي يتم من خلالها يكتسب هذه الصفة بالضرورة، وبالنظر للطبيعة الاتصالية لشبكة الانترنت والعلاقات التجارية وغيرها التي تتم بواسطتها، يمكن تخيل الكثير من الأسباب التي تساهم بوجود نشاط إجرامي في مجال تبييض الأموال، والاتجار بالمخدرات، والترويج للأنشطة الإرهابية المنظمة، ونظرا لارتباط أنشطة الاقتصاد الخفي ببعضها البعض خاصّة في مجال القمار وتجارة المخدرات، فإنه من الممكن أن يطور المجرمون عبر شبكة الانترنت آليات معقدة لتبييض الأموال عبر التحويل الإلكتروني من بنك لأخر أو من بلد لبلد أخر، يصعب من خلالها تتبع مثل هذه العمليات على الشبكة من الفنيّة، إضافة إلى تعقيد و ضعف التشريعات القانونية في مثل هذه الجرائم الممتدة.[26]

الفرع الثاني: معوقات تتعلّق بصعوبة إثبات الجريمة

تبرز أكثر فيما يأتي:

– **اتخاذ الجناة لتدابير أمنيّة:** يسعى المجرمين الالكترونيين إلى إخفاء جرائمهم وتمويهها؛ على أنها أعطال أو أخطاء في أنظمة التشغيل أو إزالة أثار الجريمة عن طريق التلاعب بقواعد البيانات والقوائم في جهاز الحاسوب والبرامج، لاسيما أنّ التخزين الالكتروني غير مرئي والبيانات كثيرة وهي مكتوبة بلغات رقمية لا تفهمها إلا الآلة ما لم تستعاد على شاشة الكمبيوتر؛ مما قد يلجأ هؤلاء المجرمون أيضاً إلى دس تعليمات خفيّة بين تلك البيانات أو استخدام الرموز أو التشفير بالنسبة لها، بحيث قد يستحيل على غيرهم الاطلاع عليها ويتعذر على جهات التحري والضبط الوصول إلى كشف أفعالهم غير المشروعة، بالإضافة إلى قيام مجرمي الانترنت إلى إخفاء هويّاتهم وانتحال شخصيات أخرى.

– **الطبيعة غير المادية للأدلة المستخرجة من الوسائل الالكترونية:** يكون الدليل التقليدي مرئي مثل السلاح الأبيض أو الناري أو الأداة الحادّة أو المادّة السامّة أو الوثائق والمحررات وغيرها، وهذا لا يمثّل صعوبة في الإثبات إنما يقع الإشكال في الجريمة المعلوماتية كون أدواتها غير ماديّة وغير ملموسة، تتمثّل في برامج وروابط الكترونية وتقع على التجارة الالكترونية أو العمليات المصرفية أو على أعمال الحكومة الالكترونية، إذ أنّ الجريمة المعلوماتية يكون محلّها جوانب معنوية تتعلق بالمعالجة الآلية للبيانات.

– **صعوبة الوصول إلى الدليل:** من خلال قيام مجرمي الانترنت بحماية مواقعهم وأجهزتهم بكلمات سرية أو رموز وشفرات لإعاقة المحاولات الهادفة إلى الوصول إليها أو الاطلاع عليها أو استنساخها.

بالإضافة إلى انه حينما يتوجه أفراد الضبطية القضائية من اجل القبض على الجاني و تحرير الأدلة ومنها جهاز الكمبيوتر المستخدم في الاتصال بالشبكة وما يحويه من برامج ومعلومات، إذ تثور مشكلة معرفة الرقم السري والذي بدونه لا يعمل جهاز الكمبيوتر وفي هذه الحالة لا يجوز لأجهزة التفتيش إجبار المتهم على الإفشاء عن الرقم السري لأن ذلك يعد أجراء غير قانوني، كذلك قد يتمكن الجاني من تدمير

البيانات الموجودة والمخزنة في جهاز الكمبيوتر في ثوان أثناء إجراء التفتيش، ففي هذه الحالات تكون هناك صعوبة في جمع الأدلة المادية التي تثبت ارتكاب جرائم الانترنت.[27]

– **سهولة محو الدليل الرقمي أو تدميره في زمن قصير جدا:** يعبّر عن ذلك بخاصيّة تطاير البيانات، فالأدلّة الرقمية وبحكم أنها بيانات معبر عنها بلغة الآلة والأرقام، إلاّ انه يمكن التلاعب بها وإخفائها بسهولة، حيث يقوم الجاني بمحو وتدمير أدلة الإدانة التي تكون قائمة ضدّه بسهولة متناهية أي تدميرها في زمن قصير جدا.

– **ضخامة حجم المعلومات والبيانات المتعين فحصها:** إذا كانت سلطات التحقيق في الجرائم التقليدية أمام مسرح جريمة واضح محدد المعالم يمكنهم التحقيق فيه، فإنهم في حالة الجريمة المعلوماتية سيكونون أمام عالم افتراضي لا متناهي متباعد الأطراف متصل ببعضه البعض؛ من حيث المعلومات والأجهزة وحتى الكم الهائل والضخم والرهيب من البيانات والمعطيات الواردة فيه، وبالتّالي فإنّ هؤلاء المحققين لن يستطيعوا بأية حال من الأحوال التحقيق والتثبت في كل تلك البيانات والمعلومات، لأنه عمل شاق ومرهق أمام قلّة الإمكانات المادية والبشرية المساعدة، الأمر الذي يشكّل عائقاً أمام كشف الجريمة المعلوماتية والبحث والتحري فيها، إذ أنّ مجرّد طباعة كل ما يوجد على الدعامة الممغنطة لمركز حاسب متوسط الأهميّة يتطلّب مئات الآلاف من الصفحات، التي قد لا تثبت كلّها تقريباً شيئاً على الإطلاق، فلا ربما قام المحقّقون بالتحقيق في جريمة ما، تمّ يكتشفون بأنهم في مسار خاطئ ليقوموا بعدها بإعادة التحقيق من جديد في معطيات ومعلومات أخرى، وكل ذلك مردّه إلى الكم الهائل من المعطيات والبيانات والمواقع وعدم وجود آليّات لفرزها بالإضافة إلى إشكالية البعد الجغرافي بين كل من مرتكب الجريمة والضحية.[28]

المطلب الثاني: مظاهر تعود لأسباب بشرية

تنقسم هذه المعوقات إلى معوّقات متصلة بالمجني عليهم (**الفرع الأول**) ومعوقات مرتبطة بالجهات التي تتولى التحقيق في الجرائم المعلوماتية (**الفرع الثاني**).

الفرع الأول: المعوقات المتّصلة بالمجني عليهم

تتلخص فيما يلي:

– **تكتّم المجني عليهم وإحجامهم عن الإبلاغ على الجرائم المعلوماتية:** يمثل تكتّم المجني عليهم وإحجامهم في الإبلاغ عن الجرائم المعلوماتية من أكثر الصعوبات التي تكتنف عملية البحث والتحري عن الجريمة المعلوماتية، وذلك يعود لعدّة عوامل يمكن أن نذكر منها خوف الجهات المتضررة من الإبلاغ عن الجريمة؛ خشية كشف نظام حمايتها الضعيف، حتى لا تكون عرضة لعمليات إجرامية أخرى، ولا بما كذلك خوفهم من عمليات التفتيش التي تقوم بها جهات التحقيق وما يمثله ذلك من كشف لأسرارهم أو الاطلاع على معلومات وبيانات يتكتّمون عن الإفصاح عنها ولا ترغب المؤسسات المتضرّرة الكشف عنها، هذا بالإضافة إلى خشيتها من تضرر سمعتها في السوق وهو ما يؤدي إلى عزوف الزبائن من

التعامل معها ونقص ثقتهم في نظام الحماية الخاص بتلك المؤسسات، كذلك جهل المجني عليهم من أنّ تلك الهجمات الالكترونية هي أعمال إجرامية معاقب عليها في القانون أو عدم ثقتهم في جهات التحقيق.

– **اهتمام الشركات والمؤسسات بالجانب الترويجي والتسويقي لمنتجاتها وتحقيق الأرباح وإهمالها للجانب الأمني:** رغبة من مختلف الشركات في بيع منتجاتها والحصول على أكبر قدر ممكن من الأرباح فإنها تلجأ إلى تبسيط الإجراءات وتسهيل استخدام البرامج والأجهزة وملحقاتها وزيادة المنتجات واقتصار ها على تقديم الخدمة وعدم التركيز على الجانب الأمني.

– **عدم إدراك خطورة الجرائم المعلوماتية من قبل المجني عليهم:** كما أسلفنا سابقاً فإنّ جهل الأفراد والمؤسسات بمدى خطورة الجرائم المعلوماتية، يجعلهم يتهاونون في الإبلاغ عنها ولا يتخذون احتياطاتهم لتفادي وقوعهم ضحايا لتلك الجرائم، كتامين شبكاتهم وأجهزة الحاسوب التي يستعملونها، ويتركونها عرضة للاختراق ولسرقة البيانات منها حتى دون أن يدركوا ذلك.

الفرع الثاني: معوقات قضائية

تتمثل المعوقات المرتبطة بالجهات القضائية التي تتوّلى التحقيق في:

– **نقص خبرة جهات البحث والتحري والتحقيق في الجرائم المعلوماتية:** تواجه عملية استخلاص الدليل في الجرائم المعلوماتية صعوبات جمّة، مثل نقص الخبرة لدى رجال الضبط القضائي أو أجهزة الأمن بصفة عامّة، وكذلك لدى أجهزة العدالة الجنائية ممثلة في سلطات الاتهام والتحقيق الجنائي.

لهذا فإنّ عملية البحث والتحقيق في جرائم المعلوماتية هي في غاية الأهمية والصعوبة، لاسيما بالنظر للتكوين العلمي والتدريبي والخبرات المكتسبة لرجال الضبط القضائي وسلطات التحقيق الجنائي والحكم، وذلك لأنّ حداثة الجرائم وتقنياتها العالية تتطلب من القائمين على البحث الجنائي والتحقيق إلمام كاف بها فلا يكفي أن يكون لهم الخلفية القانونية أو أركان العمل الشرطي فقط، ولكن لا بدّ من الإلمام بخبرة فنية في مجال الجريمة المرتكبة بواسطة الانترنت ومن أجل ذلك، فإنه لا بدّ من إيجاد أسلوب خاص للتحقيق في تلك الجرائم يجمع بين الخبرة الفنية والكفاءة المهنية، ومن الممكن لتحقيق ذلك إتباع الخطوات التالية:

– تبادل المعلومات بين المحقق وخبير الحاسوب وذلك قبل البدء في التحقيق، وأخذ أقوال الشهود والمشتبه فيهم أو استجواب المتهمين[29]، حيث يغطّي كل طرف النقص الموجود لدى الطرف الأخر، أو يكمّل له المهمة التي يريد القيام بها أو من المطلوب منه القيام بها حتى يتفادوا التناقض.

– حصر النقاط المطلوب استجلائها من قبل الخبير والمحقّق قبل البدء في التحقيق ليتولى المحقق بعد ذلك ترتيب تلك النقاط.

– أخذ أقوال الشهود واستجواب المتّهمين من قبل المحقق وبحضور الخبير، الذي يجوز له توجيه الأسئلة التقنية التي لا يدركها المحقق والتي من الممكن أن تكشف الإجابة عنها خيوط الجريمة.

– التنسيق بين المحقق والخبير في الحصول على البيانات المخزنة في الحاسوب الآلي وملحقاته الخاصة بالشاهد أو المتهم الذي يتم التحقيق معه.

– الاستعانة بالتقنيات المتطوّرة في المجال المعلوماتي في مواجهة الجرائم المعلوماتية؛ لاسيما وأنّ هذه التقنيات أثبتت جدارتها ونجاحها في جمع الأدلة الجنائية وصناعة البنية الاتهامية وتحليل القرائن واستنتاج الحقائق.

المطلب الثالث: معوقات مرتبطة بالجانب القضائي

تصطدم مسألة إثبات الجرائم المعلوماتية، بالعديد من المعوّقات والمسائل الهامّة على الصعيد القضائي، تتمثّل أساساً في انعدام وجود آليات مرنة للتعاون الدولي في المجال الجنائي لمواجهة الجرائم المعلوماتية، بحكم أنها جرائم من طبيعة خاصة تتطلب عملية مواجهتها تكاثف الجهود وتنسيقها على المستوى الدولي (**الفرع الأول**) بالخصوص عندما تصطدم أغلبية إجراءات التحقيق المتّبعة في هذه الجرائم بعقبات قانونية على غرار مسالة الاختصاص (**الفرع الثاني**).

الفرع الأول: قصور التعاون الدولي في مجال مكافحة الجرائم المعلوماتية

باعتبارها لا تعترف بالحدود الإقليمية لكل دولة ويمكن ارتكابها عن بعد، صارت الجريمة المعلوماتية محل جدل مثار بين عدّة دول في النظام القانوني المطبّق عليها، لهذا فإنّ التعاون الدّولي في مجال مكافحة هذا النوع من الجرائم وإثباتها يعدّ مسألة هامّة وحاسمة ولكنّها في نفس الوقت مسألة معقّدة لأسباب عدّة نذكر منها:

– **صعوبة توحيد المفاهيم:** لابدّ أن يؤسس أي تعاون دولي على مفاهيم موحّدة غير مختلف عليها، وهو أمر لا نجده في حالة الجريمة المعلوماتية، إذ هي لحد الآن محل اختلاف بين مختلف الأنظمة القانونية بالإضافة إلى أنّ عالم الإجرام المعلوماتي ينطوي على الكثير من المصطلحات التقنية الغير مستقرة بسبب تغير واختلاف مفاهيمها وتجدّدها المتطور.

إنّ اختلاف المفاهيم المرتبطة بالجرائم المعلوماتية بين نظام قانوني وأخر، يضعف من منظومة القانون الدولي في ضبط تلك الجرائم وبالتالي يسهل على الجناة الإفلات من المسائلة الجنائية، وتعتبر قضية الدودة الحاسوبية " **لوف باغ love bug** " التي أدّت في الفلبين سنة 2000 إلى تعطيل ملايين الحواسيب في أنحاء العالم، أحسن مثال على اختلاف الأنظمة القانونية بين الدول، حيث وجدت أعمال التحقيق المتخذة للكشف عن القضية صعوبات كثيرة، بسبب أنّ الفلبين لم تكن تجرم العمل الضار والمؤذي بشكل كاف[30].

– **تنوع واختلاف الأنظمة الإجرائية:** التعاون الدولي لا يقتصر على الجانب الموضوعي بل يتعداه إلى التعاون الإجرائي بين مختلف الدول، لأنّ التعاون في حد ذاته يتطلّب إيجاد وسائل إجرائية وآليات يتم من خلالها، وأنه من شأن الاختلاف الموجود بين الأنظمة الإجرائية للدّول أن تصعّب من مسألة التعاون.

إنّ التعاون في المسائل الإجرائية هو من أهم المسائل في مكافحة الجرائم المعلوماتية، خاصّة وأنّ هذه الجرائم وبسبب طبيعتها وسرعة ارتكابها أو سهولة إخفاء الأدلة الناتجة عنها، يتطلّب ذلك من مختلف الأنظمة القانونية الإجرائية، أن تكيّيف الإجراءات التقليدية المتبعة من طرفها في التحقيق والمحاكمة بما يتوافق مع تلك الطبيعة والسرعة.

ففي أغلب الأحيان ما تختلف طرق وإجراءات التحري والتحقيق في دولة ما عنها في دولة أخرى، وهي إجراءات وإن كانت تثبت فاعليتها في دولة ما، قد لا تكون مرخّص بها أصلاً كما هو الحال مثلاً بالنسبة للمراقبة الالكترونية.

نشير إلى أن اتفاقية بودابست لمواجهة الجريمة المعلوماتية قد نصت على وجوب التعاون بين أطراف الاتفاقية مع بعضها البعض وفقا لأحكام هذا الفصل، في تطبيق الأصول الدولية المتصلة بالتعاون الدولي في المواد الجنائية، والاتفاقيات المعتمدة على التشريعات المتماثلة أو النظيرة والقوانين المحلية، إلى أوسع نطاق ممكن، لأغراض التنقيب والتحري أو الإجراءات الجنائية المتعلقة بالجرائم الجنائية المرتبطة بنظم وبيانات معلوماتية أو لجمع أدلة ذات شكل اليكتروني للجريمة الجنائية.[31]

الفرع الثاني: إشكالية الاختصاص القضائي

قواعد القانون الجنائي (بشقيه الموضوعي والإجرائي)، تخضع في تطبيقها من حيث المكان لمبدأ مستقر ومعروف ألا وهو مبدأ الإقليمية الذي يعني خضوع الجرائم التي تقع في إقليم دولة معينة لقانونها الجنائي النافذ، بحيث تصبح محاكمها هي صاحبة الولاية بنظر الدعوى الناشئة عنها؛ ولا تخضع من حيث الأصل لسلطان أي قانون أجنبي وفي المقابل لا يمتد سريان قانون الدولة الجنائي خارج نطاقها الإقليمي وفقاً لحدودها المعترف بها في القانون الدولي إلاّ في أحوال استثنائية اقتضتها حماية المصالح الجوهرية للدّولة أو متطلبات التعاون الدولي في مكافحة الإجرام.[32]

كما هو معلوم فإنّ الشبكة العنكبوتية لا تستأثر بها دولة بعينها، حيث يتسنى لمستخدميها ولوجها من أية موقع في العالم تقريباً من خلال حاسوب يكون متصلا بها، فهي بطبيعتها لا تحدّها حدود ومن تمّ تكون من حيث المبدأ خارج أية رقابة أو سيطرة من أية جهة، وهذا يستتبع عدم إمكان خضوعها لسلطان قانون جنائي معين.

فجريمة السب مثلاً عبر الرسائل الالكترونية email تقع أحياناً في بلد ويتلقّاها الضحية في بلد أخر، وهنا ينبغي أن نشير إلى أنّ هذه الرسائل وغيرها من أدوات الاتصال عن بعد بواسطة هذه الشبكة، تمرّ في كثير من الأحيان بأكثر من دولة قبل وصولها إلى بلد الاستقبال، ناهيك أنّ بعض الأفعال التي تبثه من خلال الانترنت تعدّ أحياناً جريمة في بلد ومباحة في غيره من البلدان المرتبطة بهذه الشبكة.

لتوضيح أكثر حول قضايا السب والشتم عبر البريد أو الرسائل الإلكترونية نورد هذه القضية: واقعة المحضر 2ح قسم المصنفات الفنية فى ديسمبر 2008م (**تشهير وسب وقذف**) بشأن قيام مجهول

باختراق البريد الالكتروني الخاص بالمجني عليها وسرقة محتوياته من صور خاصة بها وبيانات أصدقائها ومراسلات شخصية هامة ، ونشر ذلك على موقع فيس بوك وإضافة عبارات تسيء لسمعتها وإضافة رقم هاتفها المحمول.

أسفر الفحص الفني للموقع والرسائل التي أرسلها مرتكبي الواقعة لأصدقاء المجني عليها عبر البريد الالكتروني إلى تحديد الجهاز المستخدم في الواقعة ومالكه ورقم تليفونه الأرضي وبإجراء التحريات السرية التقليدية أسفرت عن تحديد مرتكب الواقعة (مستخدم جهاز الحاسب المنوه عنه بمحضر الفحص الفني) وضبطه وضبط جهاز الحاسب المستخدم في ارتكاب الواقعة.

مع العلم أن المجني عليها من مدينة طنطا وجهاز الحاسب الآلي مرتكب الواقعة في مدينة طلخا بالدقهلية بمصر.[33] وما يزيد من حدّة المشكلة انعدام أو ضعف الرقابة على الرسائل الالكترونية، وغياب قانون محدّد يجري إعماله على مثل هذه الأفعال، ما من شأنه أن يبعث على التساؤل عن القانون الواجب التطبيق على الموقع الالكتروني على شبكة الانترنت.[34]

وإعمالاً لمبدأ إقليميّة النص الجنائي فإنّ الأفعال الموصوفة بأنها جريمة معلوماتية عابرة للحدود تخضع لاختصاص أكثر من دولة، فإذا وقع السلوك في نطاق بلد أخر فإنّ كلا البلدين يجب عليهما إعمال قانونهما على الواقعة، أي أنه يتم تطبيق قانون كل دولة تحقّق في نطاقها أحد عناصر الركن المادّي للجريمة، فيكفي ليكون قانون البلد واجب التطبيق تلقّي الضحيّة الرسالة الالكترونية المجسّدة لجريمة السب أو التهديد مثلاً في نطاقه ولو كان الفعل ذاته غير معاقب عليه في بلد المنشأ.

كما يجب التنويه إلى أنّ اختلاف وتباين المعايير الوطنية فيما يتعلّق بتحديد الاختصاص، يصعّب من عملية البحث والتحري ويفضي إلى حدوث تنازع في الاختصاص بشأن هذه الطائفة من الجرائم.

فمثلاً لو أنّ شخصاً ارتكب أياً من الجرائم المعلوماتية على إقليم دولة لا يحمل جنسيتها؛ فقد يحدث التنازع بين قانون الدولة التي ارتكبت الجريمة على إقليمها وقانون الدولة التي ينتمي إليها، ففي هذه الحالة الفعل يتنازعه قانونان، الأوّل هو قانون دولة الإقليم على أساس مبدأ الإقليمية، وفي الوقت ذاته قد يخضع لقانون دولة الجاني عملاً بمبدأ الشخصية الايجابية، ليس هذا فحسب بل قد ينعقد الاختصاص لدولة ثالثة متى كانت الجريمة ماسّة بمصالحها الحيوية وفقاً لمبدأ العينية.

حتى لو تمّ افتراض إمكانية إيجاد حل لهذه المشكلة من الزاوية القانونية، فإنها تظل تصطدم بعقبات عملية بالنظر إلى الإجراءات المعقدة والطويلة التي يلزم إتباعها لمحاكمة الجاني الذي ارتكب أياً من هذه الجرائم، وكانت إقامته خارج البلد الذي تتم فيها محاكمته والأمر ينسحب كذلك على تنفيذ الأحكام الصادرة بالخارج، ومن الصعوبات في ذلك هو مبدأ عدم جواز محاكمة الشخص عن الفعل الواحد مرّتين وكذلك جواز تسليم الوطنيين.

من خلال كل ذلك يمكن القول أنّ الجرائم المعلوماتية لا تحدّها حدود عكس الجريمة التقليدية المعروفة، الأمر الذي يجعلها في كثر من الأحيان تستعصي على الخضوع للقوالب القانونية التي تحكم مسألة الاختصاص المكاني، ومن تمّ فإنّ الطبيعة الخاصّة لهذا النوع من الجرائم الغير تقليدية تقتضي تجاوز القوالب والمعايير التي طرحها الفقه للتغلب على مشكلة تنازع الاختصاص والعمل على تبني حلول أكثر مرونة تأخذ في الحسبان النطاق الجغرافي؛ لهذه الجرائم وسهولة ارتكابها وآلية اقترافها والتخلص من أثارها وما إلى ذلك من اعتبارات يفرضها الطابع التقني المتطور لها.

خاتمة:

إنّ تزايد ارتكاب الجريمة المعلوماتية وتجاوز نتائجها السلبية حدود الدول والحكومات، أثار عدد من الإشكالات القانونية من الناحية الإجرائية تمثّلت في المقام الأوّل في بعض المعوّقات التي تحيط باكتشاف وإثبات هذه الجرائم وقبول الدليل بشأنها بسبب اعتبارها لا تترك أثرا مادياً ملموساً كما هو الحال في الجرائم التقليدية.

بالإضافة إلى ما يثيره ذلك من عقبات تواجه الأجهزة القضائية والأمنية من أجل مباشرة بعض الإجراءات عابرة للحدود؛ كالمعاينة والتفتيش والخبرة في البيئة الرقمية أو الافتراضية، زد على ذلك مشكلة تنازع الاختصاص بصدد هذه الجرائم لأنّ أثارها تتجاوز الحدود الجغرافية للدول، الأمر الذي يجعل جهود الدول منفردة في سبيل مكافحتها أمراً غير مجدي، وتضل مشوبة بالقصور وعدم النجاعة والفاعلية.

لهذا حاولنا من خلال مقالنا هذا تبيان الخصائص والميزات التي تنفرد بها الجريمة المعلوماتية في جانب التحقيق، وكذا الصفات التي من المفروض أن يتحلى بها الشخص الذي يتصدى للتحقيق في مثل هذا النوع من الجرائم.

تطرّقنا كذلك إلى أساليب البحث والتحري التقليدية وكيفية توظيفها في مجال التحقيق في الجريمة المعلوماتية، بالإضافة إلى الأساليب التي استحدثها المشرع الجزائري في مجال مكافحة الإجرام المعلوماتي وما يمكن أن يواجه المحققين وأجهزة البحث والتحري من صعوبات نظراً لخصوصية هذه الجريمة.

بناءاً على ذلك فإنّ أهم ما توصلنا له من نتائج من خلال دراستنا لإجراءات البحث والتحري في الجريمة المعلوماتية تتمثل فيما يلي:

1- الطبيعة الخاصة للجريمة المعلوماتية الأمر الذي دعى المشرع الجزائري إلى إعادة تقييمه لبعض القواعد الإجرائية المتاحة في استخلاص الدليل كالتفتيش والخبرة مثلا؛ وجعلها مناسبة أو موافقة للاستعمال في مجال البيئة الرقمية، وهو ما حدث فعلاً بموجب القانون 04/09 المتعلّق بالقواعد الخاصّة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، فضلاً عن استحداث نوع أخر من القواعد الإجرائية تتوافق مع الطبيعة الخاصة للجريمة المعلوماتية مثل اعتراض المراسلات والتسرب والمراقبة الالكترونية.

2- الدليل الأنسب في إثبات الجريمة المعلوماتية هو الدليل الرقمي.

3- الدليل الرقمي على ضوء ما أسفرت عليه التطورات التقنية في مجال المعلوماتية، يحوز على صفة الشرعية في حالة ما إذا تمّ بوسائل قانونية ولم يتم التلاعب به عن طريق التغيير والتحريف والتعديل.

4- يجب التفريق في مسألة تقدير القيمة القانونية للدليل الرقمي بين أمرين مهمين هما: القيمة العلمية القاطعة للدليل الرقمي وكذا الظروف والملابسات التي تحيط بهذا الدليل.

5- سهولة العبث بالدليل المعلوماتي من خلال محوه وتدميره وتغييره.

6- التكاليف العالية لعمليات التحري عبر الانترنت.

هذا بالنسبة للنتائج المستنتجة والمتوصل إليها من خلال هذا المقال، أمّا من ناحية التوصيات المقترحة والتي نراها ربما كفيلة في تعزيز مجال البحث والتحري عن الجريمة المعلوماتية و تحسينه أكثر مما هو عليه الآن و التقليل من الإشكالات التي يتعرض لها رجال الضبط القضائي في هذا المجال فإنّ نوصي بما يلي:

1- إعادة النظر أكثر في القوالب الإجرائية الحالية بما يتلاءم وطبيعة الجريمة المعلوماتية.

2- الدعوة إلى تعزيز التعاون بين الأنظمة القضائية والشرطية لمواجهة التحديات الإجرائية الناجمة عن الجريمة المعلوماتية.

3- الاهتمام أكثر بتأهيل كوادر الأجهزة القضائية والأمنية بما يجعلها قادرة على التعامل مع هذه الجرائم بكفاءة واقتدار.

4- الدعوة إلى إنشاء ضبطية قضائية بالإضافة إلى نيابة عمومية مختصة في مجال الجرائم المعلوماتية.

---

[1] - نبيل صقر، جرائم الكمبيوتر والانترنت في التشريع الجزائري، موسوعة الفكر القانوني، دار الهلال للخدمات الإعلامية، الطبعة الأولى 2005، الجزائر، ص 59.

[2] - سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة مقدمة لنيل شهادة الماجستير في العلوم القانونية تخصص علوم جنائية، جامعة الحاج لخضر باتنة كلية الحقوق والعلوم السياسية، السنة الجامعية 2012-2013، ص143.

[3] - هلالي عبد الله أحمد، تفتيش نظم الحاسوب الآلي وضمانات المتهم المعلوماتي، الطبعة الأولى، دار النهضة العربية، القاهرة، سنة 1997، ص73.

[4] - أنظر المادة 47 من قانون الإجراءات الجزائية الجزائري.

[5] - أنظر المادة 335 من قانون العقوبات الجزائري.

[6] - أنظر المادة 44 من قانون الإجراءات الجزائية الجزائري.

[7] - ساغي امحمد، العقبات الإجرائية في إثبات الجريمة المعلوماتية، مذكرة تخرج لنيل شهادة ماستر تخصص إدارة أعمال، جامعة خميس مليانة، كلية الحقوق والعلوم السياسية، السنة الجامعية 2013-2014، ص 67.

[8] - المادة 05 من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، المؤرخ في 05 أوت 2009، الصادر بالجريدة الرسمية للجمهورية الجزائرية رقم 47 الصادرة بتاريخ 16 غشت 2009.

[9] - حسين بن سعيد بن سيف الغفاري، التحقيق وجمع الأدلة في الجرائم المتعلقة بشبكة الانترنت، مقال منشور في موقع: www.minshawi.com

crimes dans dans les informatiques et d’autres‹ crimes‹les‹ Spreutels .[10]- Jean P
inter de- dr pen 1993- p170. - domaines de le technologie informatique en Belgique- rev

[11] - نوارة باشوش، مقال منشور في جريدة الشروق اليومي الجزائرية، يوم 2011/06/19، تاريخ الإطلاع عليه يوم 28 جانفي 2015 عبر الرابط التالي: http://www.echoroukonline.com

[12] - عبد الحميد السواري، التزوير والتزييف مدنيا وجزائيا في ضوء الفقه والقضاء، منشأة، مصر 1996، ص552.

[13]

[14] - سعيداني نعيم، مرجع سابق، ص165.

[15] - ساغي امحمد، مرجع سابق، ص 89.

[16] - voirchef la criminalité loi de 28 novembre 2000 relative a meumier (c) la information rev- art. pem. Crim. 2002 p 611.

[17] -meumier. (c) . art. prec. p 681.

[18]- محمد أو العلاء عقيدة، مراقبة المحادثات التلفونية، دراسة مقارنة، دار النهضة العربية، 2008، ص 192.

[19] - - سعيداني نعيم، ص184.

[20] - نفس المرجع، ص 184.

[21] - هلالي عبد الله احمد، حجية المخرجات الكومبيوترية في المواد الجنائية، الطبعة الثانية، دار النهضة العربية، 2008، ص 104، - سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، ص207.

[22] - علي حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والانترنت، عالم الكتب الحديثة، الأردن، ص 186.

[23] - - سعيداني نعيم، مرجع سابق، ص 222.

[24] - أنظر المادتين 339 و 341 من قانون العقوبات الجزائري.

[25] - نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، الطبعة الأولى 2008، الأردن، ص 54.

[26] - صغير يوسف، الجريمة المرتكبة عبر الانترنت، مذكرة لنيل شهادة الماجستير في القانون تخصص القانون الدولي للأعمال، جامعة مولود معمري تيزي وزو، كلية الحقوق والعلوم السياسية، الموسم الجامعي 2013/2012، ص127.

[27] - عمرو عيسى الفقي، الجرائم المعلوماتية، (جرائم الحاسب الآلي والانترنت في مصر والدول العربية)، المكتب الجامعي الحديث، الطبعة الأولى 2006، مصر، ص93.

[28] - سليمان بن مهجع العنزي، وسائل التحقيق في جرائم نظام المعلومات، رسالة ماجستير في العلوم الشرطية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض، 2003، ص 98.

[29] - united nation manual on the prevention and control of computer. related crime vienna 1999.

[30] - مؤتمر الأمم المتحدة الثاني عشر لمنع الجريمة والعدالة الجنائية، البند الثامن من جدول الأعمال المؤقت التطورات الأخيرة في استخدام العلم والتكنولوجيا من جانب المجرمين والسلطات المختصة في مكافحة الجريمة بما فيها الجرائم الحاسوبية، المنعقد بالبرازيل ما بين الفترة الممتدة من 12 إلى 19 أفريل سنة 2010 رقم a /conf 213/09، ص 16.

[31] - هلالي عبد الله أحمد، جرائم المعلوماتية عابرة للحدود (أساليب المواجهة وفقا لاتفاقية بودابست)، دار النهضة العربية، الطبعة الأولى 2007، مصر، ص66.

[32] - على احمد راشد، المدخل وأصول النظرية العامة 1974 ص 185 نقلا عن موسى مسعود ارحومة، الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، المؤتمر المغاربي الأول حول المعلوماتية والقانون، أكاديمية الدراسات العليا طرابلس 28-29/ أكتوبر 2009، ص 12.

[33] - حسام نبيل الشنراقي، ورقة عمل تم تقديمها في ندوة **"الاستخدام الأمن لشبكة الانترنت "** المنعقدة في جامعة طنطا بتاريخ 2010/5/15، أطلع عليه يوم 28 جانفي 2015 عبر الرابط التالي: http://kenanaonline.com

[34] - موسى مسعود ارحومة، مرجع سابق، ص 17.